

1 Stephen R. Basser (SBN 121590)
2 Samuel M. Ward (SBN 216562)
3 **BARRACK, RODOS & BACINE**
4 One America Plaza
5 600 West Broadway, Suite 900
6 San Diego, CA 92101
7 (619) 230-0800
8 sbasser@barrack.com
9 sward@barrack.com

10 *Counsel for Plaintiff and the Proposed Class*
11 (Additional Counsel for Plaintiff Appear on Signature Page)

12 **UNITED STATES DISTRICT COURT**
13 **CENTRAL DISTRICT OF CALIFORNIA**

14 BRIAN WEBBE, individually, and on
15 behalf of all others similarly situated,

16 Plaintiff,

17 vs.

18 LOANDEPOT, INC.,

19 Defendant.

20 Case No.

21 **CLASS ACTION COMPLAINT**
22 **AND DEMAND FOR JURY TRIAL**

1 Plaintiff Brian Webbe (“Plaintiff”), individually, and on behalf of the class
2 defined below, brings this class action complaint against loanDepot, Inc. (“loanDepot”
3 or “Defendant”) and alleges as follows:

4 INTRODUCTION

5 1. Defendant loanDepot, Inc. is a nonbank holding company based out of
6 Irvine, California, which sells mortgage and non-mortgage lending products. Founded
7 in 2010, loanDepot has “grown to become the nation’s fifth largest retail mortgage
8 lender and the second largest nonbank retail originator, funding more than \$275 billion
9 since inception. Today, [loanDepot’s] nationwide team of 6,000-plus members assists
10 more than 27,000 customers each month.”¹

11 2. Between January 8, 2024 and January 22, 2024, loanDepot announced a
12 security incident during which unauthorized parties gained access to sensitive
13 personal information of approximately 16.6 million individuals in its systems (the
14 “Data Breach”).

15 3. Specifically, on or around January 8, 2024, in a Form 8-K filing² with the
16 SEC, loanDepot reported the following:

17 loanDepot, Inc. (the “Company”) recently identified a
18 cybersecurity incident affecting certain of the Company’s
19 systems. Upon detecting unauthorized activity, the Company
20 promptly took steps to contain and respond to the incident,
21 including launching an investigation with assistance from
22 leading cybersecurity experts, and began the process of
23 notifying applicable regulators and law enforcement.

24 Though our investigation is ongoing, at this time, the
25 Company has determined that the unauthorized third party
26 activity included access to certain Company systems and the
27 encryption of data. In response, the Company shut down
28 certain systems and continues to implement measures to
secure its business operations, bring systems back online and

27 ¹ <https://www.loandepot.com/about>

28 ² See <https://investors.loandepot.com/financials/sec-filings/default.aspx>

respond to the incident.³

4. On or around January 8, 2024, loanDepot also announced the following on its website:

loanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers and we are focused on resolving these matters as soon as possible.⁴

5. Around this time, loanDepot's website, including its customer portals, appeared to be non-functional, and the following error message appeared on loanDepot's customer login page, asking customers seeking to make a payment to call or mail in their payment instead:⁵

An Important Update.

loanDepot is experiencing a cyber incident that has prompted us to take certain systems offline while we respond to the matter. We are working diligently to return to normal business operations as soon as possible. Recurring automatic payments are processing as expected, but there may be a temporary delay in viewing the posted payment in your payment history. If you are seeking to make a payment, you may do so through our contact center by speaking with an agent at 866-258-6572 from 7 am CT to 7 pm CT Monday through Friday, and 8 am CT to 5 pm CT on Saturday. You may also mail your payment with your loan number to the address on your statement. We apologize for any inconvenience.

³ See loanDepot January 8, 2024 Form 8-K Filing, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/446c437f-153f-425d-adc6-bf37155d6e91.pdf> (last accessed January 25, 2024).

⁴ See loanDepot, *loanDepot is experiencing a cyber incident*, <https://loandepot.cyberincidentupdate.com/> (last accessed Jan. 25, 2024).

⁵ <https://techcrunch.com/2024/01/08/loandepot-outage-suspected-ransomware-attack>

6. On January 22, 2024, in a Form 8-K/A filing⁶ with the SEC, loanDepot further reported, “[T]he Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.”

7. On January 22, 2024, loanDepot also provided the following information on its website:

The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyloanDepot and Servicing customer portals.

Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.⁷

8. Although loanDepot has not yet shared what type of customer personal information was accessed and stolen from its systems,⁸ based on information and belief, the information likely included, among other information, the following personally identifying information (“PII”) and other financial information:

- Identifying information, such as your name, age, address, phone number and social security number
- Employment information
- Contact information (such as first and last name, mailing or property address, phone number, email address)
- Account access information, such as username and password

⁶ See loanDepot Form 8-K/A Filing; <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/80bb5ce4-2f0e-49d6-b1a1-bd5aa864f4d1.pdf> (last accessed Jan. 25, 2024).

⁷ See loanDepot, *loanDepot Provides Update on Cyber Incident*, <https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx> (last accessed Jan. 25, 2024).

⁸ See BleepingComputer, *loanDepot cyberattack causes data breach for 16.6 million people*, <https://www.bleepingcomputer.com/news/security/loandepot-cyberattack-causes-data-breach-for-166-million-people/> (last accessed Jan. 25, 2024).

- Demographic information (such as date of birth, gender, marital status, ethnicity, race)
- Social security, driver's license, passport, and other government identification numbers
- Loan account information (such as loan number)
- Bank account and credit/debit card numbers
- Other personal information needed from you to provide real estate-related, loan-related, insurance-related, credit-related, and homeownership-related services to you
- Information for fraud detection and prevention
- Financial information such as your income, assets and liabilities, as well as information about your savings, investments, insurance and business.

9. At all relevant times, Defendant was aware of the risks of a Data Breach and that it would be specifically targeted by malicious hackers. Defendant's CEO Frank Martel acknowledged as much, stating, "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers."⁹ loanDepot also suffered another data security incident in August 2022 (which it did not announce until May 2023) whereby unauthorized parties accessed documents containing its customers' personal information.¹⁰

10. Armed with the PII from these records, hackers can sell the PII to other thieves or misuse themselves to commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; or give false information to police during an arrest.

11. As a result of Defendant's willful failure to prevent the Data Breach, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience, and face an increased risk of financial harms, in that they are at substantial risk of identity theft, fraud, and other harm.

⁹ See, *supra*, n. 7.

¹⁰ <https://www.mass.gov/doc/assigned-data-breach-number-29545-loandepot-inc/download>.

PARTIES

12. Plaintiff Brian Webbe is a resident and citizen of Wayne County, Pennsylvania. Plaintiff applied for and obtained a mortgage through loanDepot in or about May 2022. Through this application, Plaintiff provided Defendant his PII. As a result of Defendant's actions, Plaintiff has been injured and has financial losses and will be subject to a substantial risk for further identity theft due to Defendant's Data Breach. Since the Data Breach, Plaintiff Webbe has monitored his financial accounts and credit reports carefully. As a further result of Defendant's actions, Plaintiff will need to continue monitor his financial accounts and credit reports and take other measures to protect himself from identity theft and fraud. Plaintiff believed, at the time of applying for his personal loan, that loanDepot would maintain the privacy and security of the PII he provided to it. Plaintiff further believes he paid a premium to loanDepot for its data security. Plaintiff would not have used loanDepot had he known that it would expose sensitive PII, making them available to identity thieves.

13. Defendant loanDepot, Inc. is a Delaware corporation with its principal place of business in Irvine, California.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This lawsuit is a class action with an amount in controversy over \$5 million, involving over 100 proposed class members, some of whom are from a different state than Defendant.

15. This Court may exercise personal jurisdiction over Defendant because they are registered to do business and have their principal places of business in California.

16. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

1 A. The Data Breach

2 17. Defendant loanDepot, Inc. is an Irvine, California-based nonbank
3 holding company which sells mortgage and non-mortgage lending products. Founded
4 in 2010, loanDepot has “grown to become the nation’s fifth largest retail mortgage
5 lender and the second largest nonbank retail originator, funding more than \$275 billion
6 since inception. Today, [loanDepot’s] nationwide team of 6,000-plus members assists
7 more than 27,000 customers each month.”

8 18. Customers believe that—at a minimum—the large sum they pay for a
9 mortgage loan buys them security and peace of mind that their sensitive information
10 will be securely stored.

11 19. In its Privacy Policy, loanDepot makes numerous promises to its
12 customers that it will maintain the security and privacy of their personal information.
13 For instance, loanDepot states the following in its Privacy Policy:

14 loanDepot® values your patronage and protecting your
15 personal information is a priority. loanDepot believes in
16 protecting the confidentiality and security of the information
17 we collect about you as a customer, potential customer,
18 former customer, job applicant, or employee. We have
adopted the following policies and procedures to safeguard
the personal information about you in our possession.¹¹

19 20. The Privacy Policy also provides that Defendant collect the following
20 information on its customers:

- 21 • Identifying information, such as your name, age, address, phone number
- 22 and social security number
- 23 • Employment information
- 24 • Contact information (such as first and last name, mailing or property
- 25 address, phone number, email address)
- 26 • Account access information, such as username and password
- 27 • Demographic information (such as date of birth, gender, marital status,
- 28 ethnicity, race)

¹¹ loanDepot, Privacy Policy, <https://www.loandepot.com/privacypolicy> (last accessed Jan. 23, 2024).

- Social security, driver's license, passport, and other government identification numbers
- Loan account information (such as loan number)
- Bank account and credit/debit card numbers
- Other personal information needed from you to provide real estate-related, loan-related, insurance-related, credit-related, and homeownership-related services to you
- Information for fraud detection and prevention
- Financial information such as your income, assets and liabilities, as well as information about your savings, investments, insurance and business.¹²

21. In a section entitled, "Safeguarding Personally Identifiable Information," loanDepot provides the following assurances to its customers:

- We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.
- We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.
- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.
- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing or developing our products or services.
- Our policy, which governs the conduct of all of our employees, requires all employees to safeguard personally identifiable information about the consumers and customers we serve or have served in the past.¹³

22. The Privacy Policy also has a section entitled, "loanDepot Security Policy," which provides the following:

¹² *Id.*
¹³ *Id.*

loanDepot takes steps to safeguard your personal and sensitive information through industry standard physical, electronic, and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.¹⁴

23. Despite all of these promises, on January 8, 2024, loanDepot allowed the Data Breach to occur whereby the personal, confidential PII of Plaintiff and Class members were viewed, disclosed to, and acquired by unauthorized parties. The Data Breach exposed the sensitive PII and financial information of approximately 16.6 million customers.

B. Personally Identifiable Information (“PII”)

24. PII is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners.

25. PII is information that can be used to distinguish, identify, or trace an individual’s identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.

26. PII does not include only data that can be used to directly identify or contact an individual (e.g., name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number, payment card numbers).

27. Given the nature of the Data Breach, it is foreseeable that the compromised PII will be used to access Plaintiff and the Class members’ financial accounts, thereby providing access to additional PII or personal and sensitive information. Therefore, the compromised PII in the Data Breach is of great value to

¹⁴ *Id.*

hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, “there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.”¹⁵ For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.

28. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the “mosaic effect.”¹⁶

29. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users’ other accounts particularly when they have easily-decrypted passwords and security questions.

30. The PII loanDepot exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users’ names.

31. Unfortunately for Plaintiff and Class members, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

¹⁵ Fed. Trade Comm’n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>> [as of June 24, 2017].

¹⁶ Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁷

32. Accordingly, Plaintiff and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individual's PII is used without his or her permission to commit fraud or other crimes.¹⁸

33. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."¹⁹

34. To make matter worse, in 2017, the FBI warned the real estate industry of a "large spike in cyberattacks specifically targeting real estate companies." The FBI said that between 2016 and 2017, it witnessed a 480% increase in cyberattacks on the real estate industry.

35. loanDepot ignored these warnings and risks and failed to invest in sufficient privacy and security protections.

36. At all relevant times, Defendant was aware of the risks of a Data Breach and that it would be specifically targeted by malicious hackers. Defendant's CEO Frank Martel acknowledged as much, stating, "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our

¹⁷ G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <<http://www.gao.gov/assets/270/262904.html>> [as of June 24, 2017].

¹⁸ Fed. Trade Comm'n, Taking Charge: What To Do If Your Identity Is Stolen (April 2013) <<https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf>> [as of June 24, 2017].

¹⁹ Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>> [as of June 24, 2017].

1 industry has not been spared. We sincerely regret any impact to our customers.”²⁰
 2 loanDepot also suffered another data security incident in August 2022 (which it did
 3 not announced until May 2023) whereby unauthorized parties accessed documents
 4 containing its customers’ personal information.²¹

5 37. As a direct and proximate result of loanDepot’s reckless and negligent
 6 actions, inaction, and omissions, the resulting Data Breach, the unauthorized release
 7 and disclosure of Plaintiff’s and Class members’ PII, and loanDepot’s failure to
 8 properly and timely notify Plaintiff and Class members, Plaintiff and Class members
 9 are more susceptible to identity theft and have experienced, will continue to experience
 10 and will face an increased risk of experiencing the following injuries, *inter alia*:

- 11 a. money and time expended to prevent, detect, contest, and repair identity
- 12 theft, fraud, and/or other unauthorized uses of personal information;
- 13 b. money and time lost as a result of fraudulent access to and use of their
- 14 financial accounts;
- 15 c. loss of use of and access to their financial accounts and/or credit;
- 16 d. money and time expended to avail themselves of assets and/or credit
- 17 frozen or flagged due to misuse;
- 18 e. impairment of their credit scores, ability to borrow, and/or ability to
- 19 obtain credit;
- 20 f. lowered credit scores resulting from credit inquiries following
- 21 fraudulent activities;
- 22 g. money, including fees charged in some states, and time spent placing
- 23 fraud alerts and security freezes on their credit records;
- 24 h. costs and lost time obtaining credit reports in order to monitor their
- 25 credit records;
- 26 i. anticipated future costs from the purchase of credit monitoring and/or

27 ²⁰ See, *supra*, n. 7.

28 ²¹ <https://www.mass.gov/doc/assigned-data-breach-number-29545-loandepot-inc/download>.

1 identity theft protection services;

2 j. costs and lost time from dealing with administrative consequences of
3 the Data Breach, including by identifying, disputing, and seeking
4 reimbursement for fraudulent activity, canceling compromised
5 financial accounts and associated payment cards, and investigating
6 options for credit monitoring and identity theft protection services;

7 k. money and time expended to ameliorate the consequences of the filing
8 of fraudulent tax returns;

9 l. lost opportunity costs and loss of productivity from efforts to mitigate
10 and address the adverse effects of the Data Breach including, but not
11 limited to, efforts to research how to prevent, detect, contest, and
12 recover from misuse of their personal information;

13 m. loss of the opportunity to control how their personal information is
14 used; and

15 n. continuing risks to their personal information, which remains subject to
16 further harmful exposure and theft as long as loanDepot fails to
17 undertake appropriate, legally required steps to protect the personal
18 information in its possession.

19 38. The risks associated with identity theft are serious. “While some identity
20 theft victims can resolve their problems quickly, others spend hundreds of dollars and
21 many days repairing damage to their good name and credit record. Some consumers
22 victimized by identity theft may lose out on job opportunities, or denied loans for
23 education, housing or cars because of negative information on their credit reports. In
24 rare cases, they may even be arrested for crimes they did not commit.”²²

25 39. Further, criminals often trade stolen PII on the “cyber black-market” for
26 years following a breach. Cybercriminals can post stolen PII on the internet, thereby

27 ²² True Identity Protection: Identity Theft Overview, ID Watchdog
28 <<http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf>> [as of Sept.
23, 2016].

1 making such information publicly available.

2 **CHOICE OF LAW ALLEGATIONS**

3 40. The State of California has sufficient contacts regarding the conduct at
4 issue in this Complaint, such that California law may be uniformly applied to the
5 claims of the proposed Class.

6 41. Defendant does substantial business in California; their headquarters is
7 located in California; and a significant portion of the proposed Nationwide Class is
8 located in California.

9 42. In addition, the conduct that forms the basis for each and every Class
10 member's claims against loanDepot emanated from Defendant's headquarters in
11 Irvine, California.

12 43. The State of California also has the greatest interest in applying its law
13 to Class members' claims. California's governmental interests include not only
14 compensating resident consumers under its consumer protection laws, but also what
15 the State has characterized as a "compelling" interest in using its laws to regulate a
16 resident corporation and preserve a business climate free of unfair and deceptive
17 practices. *Diamond Multimedia Sys. v. Sup. Ct.*, 19 Cal. 4th 1036, 1064 (1999).

18 44. If other states' laws were applied to Class Members' claims, California's
19 interest in discouraging resident corporations from engaging in the sort of unfair and
20 deceptive practices alleged in this complaint would be significantly impaired.
21 California could not effectively regulate a company like loanDepot, which does
22 business throughout the United States, if it can only ensure remuneration for
23 consumers from one of the fifty states affected by conduct that runs afoul of its laws.

24 **CLASS ACTION ALLEGATIONS**

25 45. Plaintiff brings all claims as class claims under Federal Rule of Civil
26 Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

27 **A. Nationwide Class**

28 46. Plaintiff brings all claims on behalf of a proposed nationwide class

1 (“Nationwide Class”), defined as follows:

2 *All persons who utilized LoanDepot’s title insurance,*
 3 *homeowner’s insurance, mortgages, refinancing, home*
 4 *warranties, or other closing services provided by Loan*
Depot.

5 47. **Numerosity:** The Nationwide Class is so numerous that joinder of all
 6 members is impracticable. Based on information and belief, the Nationwide Class
 7 includes millions of individuals from across the country who has their PII compromised,
 8 stolen, and published during the Data Breach. The parties will be able to identify the
 9 exact size of the class through discovery and loanDepot’s own documents.

10 48. **Commonality:** There are numerous questions of law and fact common to
 11 Plaintiff and the Nationwide Class including, but not limited to, the following:

- 12 • whether Defendant engaged in the wrongful conduct alleged herein;
- 13 • whether Defendant owed a duty to Plaintiff and members of the
- 14 Nationwide Class to adequately protect their personal information;
- 15 • whether Defendant breached their duties to protect the personal
- 16 information of Plaintiff and Nationwide Class members;
- 17 • whether Defendant knew or should have known that its data security
- 18 systems, policies, procedures, and practices were vulnerable;
- 19 • whether Plaintiff and Nationwide Class members suffered legally
- 20 cognizable damages as a result of Defendant’s conduct, including
- 21 increased risk of identity theft and loss of value of PII;
- 22 • whether Defendant violated state consumer protection statutes; and
- 23 • whether Plaintiff and Nationwide Class members are entitled to equitable
- 24 relief including injunctive relief.

25 49. **Typicality:** Plaintiff’s claims are typical of the claims of the Nationwide
 26 Class members. Plaintiff, like all proposed Nationwide Class members, had their
 27 personal information compromised in the Data Breach.

28 50. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the

1 Nationwide Class. Plaintiff has no interests that are averse to, or in conflict with, the
2 Nationwide Class members. There are no claims or defenses that are unique to Plaintiff.
3 Likewise, Plaintiff has retained counsel experienced in class action and complex
4 litigation, including data breach litigation, and have sufficient resources to prosecute
5 this action vigorously.

6 51. **Predominance:** The proposed action meets the requirements of Federal
7 Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the
8 Nationwide Class predominate over any questions which may affect only individual
9 Nationwide Class members.

10 52. **Superiority:** The proposed action also meets the requirements of Federal
11 Rule of Civil Procedure 23(b)(3) because a class action is superior to other available
12 methods for the fair and efficient adjudication of the controversy. Class treatment of
13 common questions is superior to multiple individual actions or piecemeal litigation,
14 avoids inconsistent decisions, presents far fewer management difficulties, conserves
15 judicial resources and the parties' resources, and protects the rights of each class
16 member.

17 53. Absent a class action, the majority Nationwide Class members would find
18 the cost of litigating their claims prohibitively high and would have no effective remedy.

19 54. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the
20 requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of
21 separate actions by individual class members would create a risk of inconsistent or
22 varying adjudications that would establish incompatible standards for loanDepot. First
23 loanDepot continues to maintain the PII of Nationwide Class members and other
24 individuals, and varying adjudications could establish incompatible standards with
25 respect to its duty to protect individuals' personal information; and whether the injuries
26 suffered by Nationwide Class members are legally cognizable, among others.
27 Prosecution of separate action by individual class members would also create a risk of
28 individual adjudications that would be dispositive of the interests of other class

55. **Injunctive Relief:** In addition, Defendant have acted and/or refused to act on grounds that apply generally to the Nationwide Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the personally identifiable information of Nationwide Class members, (2) fail to adequately protect their personally identifiable information, and (3) violate their rights under numerous state consumer protection laws and other claims alleged herein.

Negligence

56. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

58. Plaintiff and Nationwide Class members were required to provide Defendant with their PII. Defendant collected and stored this information including their names, Social Security numbers, payment card information, checking account and routing numbers, insurance provider information, salary information, dates of birth, addresses, and phone numbers.

60. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

1 62. Defendant has a duty to use ordinary care in activities from which harm
2 might be reasonably anticipated in connection with user PII data.

3 63. Defendant breached their duty of care by failing to secure and safeguard
4 the PII of Plaintiff and Nationwide Class members. Defendant negligently stored and/or
5 maintained its data security systems, and published that information on the Internet.

6 64. Further, Defendant by and through their above negligent actions and/or
7 inactions, breached their duties to Plaintiff and Nationwide Class members by failing to
8 design, adopt, implement, control, manage, monitor and audit its processes, controls,
9 policies, procedures and protocols for complying with the applicable laws and
10 safeguarding and protecting Plaintiff's and Nationwide Class members' PII within their
11 possession, custody and control.

12 65. Defendant further breached their duty to Plaintiff and Nationwide Class
13 members by failing to comply with the Consumers Legal Remedies Act, the Customer
14 Record's Act, the Gramm-Leach-Bliley Act, and other state and federal laws designed
15 to protect Plaintiff and Class members from the type of harm they here have suffered.
16 Such a breach by Defendant constitutes negligence per se.

17 66. Plaintiff and the other Nationwide Class members have suffered harm as a
18 result of Defendant's negligence. These victims' loss of control over the compromised
19 PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad
20 other types of fraud and theft stemming from either use of the compromised
21 information, or access to their user accounts.

22 67. It was reasonably foreseeable – in that Defendant knew or should have
23 known – that its failure to exercise reasonable care in safeguarding and protecting
24 Plaintiff's and Nationwide Class members' PII would result in its release and disclosure
25 to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it
26 to other fraudsters for their wrongful use and for no lawful purpose.

68. But for Defendant's negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Nationwide Class members, their PII would not have been compromised.

69. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

70. Plaintiff and Nationwide Class members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION

Violation of California Consumers Legal

Remedies Act, California Civil Code § 1750, *et seq.*

(On Behalf of the Nationwide Class Against Defendant)

71. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

72. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time but is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendant with notice required by California Civil Code § 1782.

73. Plaintiff and Nationwide Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

74. Plaintiff, Nationwide Class members, and Defendant has engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

75. The conduct alleged in this Complaint constitutes unfair methods of

1 competition and unfair and deceptive acts and practices for the purpose of the CLRA,
2 and the conduct was undertaken by Defendant was likely to deceive consumers.

3 76. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction
4 from “[r]epresenting that goods or services have sponsorship, approval, characteristics,
5 ingredients, uses, benefits, or quantities which they do not have.”

6 77. Defendant violated this provision by representing that they took
7 appropriate measures to protect Plaintiff’s and the Nationwide Class members’ PII.
8 Additionally, Defendant improperly handled, stored, or protected either unencrypted or
9 partially encrypted data.

10 78. As a result, Plaintiff and Nationwide Class members were induced to enter
11 into a relationship with Defendant and provide their PII.

12 79. As a result of engaging in such conduct, Defendant has violated Civil Code
13 § 1770.

14 80. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of
15 this Court that includes, but is not limited to, an order enjoining Defendant from
16 continuing to engage in unlawful, unfair, or fraudulent business practices or any other
17 act prohibited by law.

18 81. Plaintiff and Nationwide Class members suffered injuries caused by
19 Defendant’s misrepresentations, because they provided their PII believing that
20 Defendant would adequately protect this information.

21 82. Plaintiff and Nationwide Class members may be irreparably harmed and/or
22 denied an effective and complete remedy if such an order is not granted.

23 83. The unfair and deceptive acts and practices of Defendant, as described
24 above, present a serious threat to Plaintiff and members of the Nationwide Class.

25
26 **THIRD CAUSE OF ACTION**

27 **Violation of Unfair Competition Law,**

28 **California Business and Professional Code Section 17200, *et seq.***

(On Behalf of the Nationwide Class Against Defendant)

84. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

85. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

86. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq.* (“UCL”), prohibits any “unlawful,” “fraudulent” or “unfair” business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

87. By reason of Defendant’s above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff and Nationwide Class members’ PII, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

88. Defendant’s business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII of consumers has been compromised for all to see, use, or otherwise exploit.

89. Defendant’s practices were unlawful and in violation of Civil Code § 1798 *et seq.* because Defendant failed to take reasonable measures to protect Plaintiff’s and the Nationwide Class members’ PII.

90. Defendant’s business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Defendant will remain private and secure, when in fact it was not private and secure.

91. Plaintiff and the Nationwide Class members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant’s above-described wrongful actions, inactions, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII.

92. Defendant’s above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff’s and

1 Nationwide Class members' PII also constitute "unfair" business acts and practices
2 within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq.*, in that Defendant's
3 conduct was substantially injurious to Plaintiff and Nationwide Class members,
4 offensive to public policy, immoral, unethical, oppressive and unscrupulous; the gravity
5 of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

6 93. But for Defendant's misrepresentations and omissions, Plaintiff and
7 Nationwide Class members would not have provided their PII to Defendant or would
8 have insisted that their PII be more securely protected.

9 94. As a direct and proximate result of Defendant's above-described wrongful
10 actions, inactions, and omissions, the resulting Data Breach, and the unauthorized
11 release and disclosure of Plaintiff and Nationwide Class members' PII, they have been
12 injured: (1) the loss of the opportunity to control how their PII is used; (2) the diminution
13 in the value and/or use of their PII entrusted to Defendant; (3) the compromise,
14 publication, and/or theft of their PII; and (4) costs associated with monitoring their PII,
15 amongst other things.

16 95. Plaintiff takes upon herself enforcement of the laws violated by Defendant
17 in connection with the reckless and negligent disclosure of PII. There is a financial
18 burden incurred in pursuing this action and it would be against the interests of justice
19 to penalize Plaintiff by forcing him to pay attorneys' fees and costs from the recovery
20 in this action. Therefore, an award of attorneys' fees and costs is appropriate under
21 California Code of Civil Procedure § 1021.5.

22
23
24
25
26 **FOURTH CAUSE OF ACTION**

27 **Violation of California Customer Records**
28 **Act, California Civil Code § 1798.80 *et. seq.***

(On Behalf of the Nationwide Class Against Defendant)

96. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

97. “[T]o ensure that personal information about California residents is protected,” Civil Code section 1798.81.5 requires that any business that “owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

98. Defendant owns, maintains, and licenses personal information, within the meaning of section 1798.81.5, about Plaintiff and the Nationwide Class.

99. Defendant violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiff and Nationwide Class members’ personal information.

100. As a direct and proximate result of Defendant’s violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

101. As a direct and proximate result of Defendant’s violations of section 1798.81.5 of the California Civil Code, Plaintiff and the Nationwide Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

102. Plaintiff and the Nationwide Class members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

FIFTH CAUSE OF ACTION

Breach of Contract

(On Behalf of the Nationwide Class Against Defendant)

1 103. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

2 104. Plaintiff and Class members entered into a contract with Defendant for
3 the provision of title insurance or other closing services.

4 105. The terms of Defendant's privacy policy are part of the contract.

5 106. Plaintiff and Class members performed substantially all that was required
6 of them under their contract with Defendant, or they were excused from doing so.

7 107. Defendant failed to perform its obligations under the contract, including
8 by failing to provide adequate privacy, security, and confidentiality safeguards for
9 Plaintiff and Class member's information.

10 108. As a direct and proximate result of Defendant's breach of contract,
11 Plaintiff and Class members did not receive the full benefit of the bargain, and instead
12 received title insurance or other closing services that were less valuable than described
13 in their contracts. Plaintiff and Class members, therefore, were damaged in an amount
14 at least equal to the difference in value between that which was promised and
15 Defendant's deficient performance.

16 109. Also, as a result of Defendant's breach of contract, Plaintiff and Class
17 members have suffered actual damages resulting from the exposure of their personal
18 information, and they remain at imminent risk of suffering additional damages in the
19 future.

20 110. Accordingly, Plaintiff and Class members have been injured by
21 Defendant's breach of contract and are entitled to damages and/or restitution in an
22 amount to be proven at trial.

23
24
25
26 **SIXTH CAUSE OF ACTION**

27 **Unjust Enrichment**

28 (On Behalf of the Nationwide Class Against Defendant)

111. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

112. Defendant received a benefit from Plaintiff and the Class in the form of payments for title insurance or other closing services.

113.

114. The benefits received by Defendant were at Plaintiff's and the Class's expense.

115. The circumstances here are such that it would be unjust for Defendant to retain the portion of Plaintiff's and the Class's payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class members' personal information.

116. Plaintiff and the Class seek disgorgement of Defendant's ill-gotten gains.

SEVENTH CAUSE OF ACTION

Invasion of Privacy

(On Behalf of the Nationwide Class Against Defendant)

117. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

118. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

119. Plaintiff and Class members have a legally protected privacy interest in their PII that Defendant required them to provide and allow them to store.

120. Plaintiff and Class members reasonably expected that their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

121. Defendant unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

122. In failing to adequately secure Plaintiff's and Class members' PII, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

123. Defendant violated Plaintiff's and Class members' right to privacy under the common law as well as under state and federal law, including, but not limited to, the California Constitution, Article I, Section I.

124. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff's and Class members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

EIGHTH CAUSE OF ACTION

Breach of Implied Contract

(On Behalf of the Nationwide Class Against Defendant)

125. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

126. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services. By providing their PII, and upon Defendant's acceptance of such information, Plaintiff and all Class Members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts.

127. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiff's and other Class Members' PII. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their Privacy Policy and other public statement described above.

1 128. Plaintiff and Class Members paid money, or money was paid on their
2 behalf, to Defendant in exchange for services, along with Defendant's promise to
3 protect their PII from unauthorized disclosure.

4 129. In their written Privacy Policy, loanDepot expressly promised Plaintiff
5 and Class Members that it would only disclose PII under certain circumstances, none
6 of which relate to the Data Breach.

7 130. Implicit in the agreement between Plaintiff and Class Members and the
8 Defendant to provide PII was Defendant's obligation to (a) use such PII for business
9 purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized
10 disclosures of the PII; (d) provide Plaintiff and Class Members with prompt and
11 sufficient notice of any and all unauthorized access and/or theft of their PII; (e)
12 reasonably safeguard and protect the PII of Plaintiff and Class Members from
13 unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept
14 such information secure and confidential.

15 131. Without such implied contracts, Plaintiff and Class Members would not
16 have provided their PII to Defendant.

17 132. Plaintiff and Class Members fully performed their obligations under the
18 implied contract with Defendant; however, Defendant did not.

19 133. Defendant breached the implied contracts with Plaintiff and Class
20 Members by failing to reasonably safeguard and protect Plaintiff's and Class
21 Members' PII, which was compromised as a result of the Data Breach.

22 134. As a direct and proximate result of Defendant's breach of the implied
23 contracts, Plaintiff and other Class Members have suffered a variety of damages
24 including but not limited to: the lost value of their privacy; they did not get the benefit
25 of their bargain with Defendant; they lost the difference in the value of the secure
26 lending services Defendant promised and the insecure services received; the value of
27 the lost time and effort required to mitigate the actual and potential impact of the Data
28 Breach on their lives, including, inter alia, that required to place "freezes" and "alerts"

1 with credit reporting agencies, to contact financial institutions, to close or modify
 2 financial accounts, to closely review and monitor credit reports and various accounts
 3 for unauthorized activity, and to file police reports; and Plaintiff and other Class
 4 Members have been put at an increased risk of identity theft, fraud, and/or misuse of
 5 their PII, which may take months if not years to manifest, discover, and detect.

6 **NINTH CAUSE OF ACTION**

7 **Breach of Fiduciary Duty**

8 (On Behalf of the Nationwide Class Against Defendant)

9 135. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

10 136. In light of their special relationship, Defendant has become the guardian
 11 of Plaintiff's and Class Members' PII and/ PHI. Defendant has become a fiduciary,
 12 created by its undertaking and guardianship of its customers' PII, to act primarily for
 13 the benefit of its customers, including Plaintiff and Class Members. This duty included
 14 the obligation to safeguard Plaintiff's and Class Members' PII and to timely notify
 15 them in the event of a data breach.

16 137. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class
 17 Members upon matters within the scope of its relationship. Defendant breached its
 18 fiduciary duties owed to Plaintiff and Class Members by failing to properly encrypt
 19 and otherwise protect the integrity of the system containing Plaintiff's and Class
 20 Members' PII.

21 138. As a direct and proximate result of Defendant's breaches of its fiduciary
 22 duties, Plaintiff and Class Members have suffered and will suffer injury, including but
 23 not limited to (a) actual identity theft; (b) an increased risk of identity theft, fraud,
 24 and/or misuse of their PII; (c) the loss of the opportunity of how their PII is used; (d)
 25 the compromise, publication, and/or theft of their PII; (e) out-of-pocket expenses
 26 associated with the prevention, detection, and recovery from identity theft and/or
 27 unauthorized use of their PII; (f) lost opportunity costs associated with the effort
 28 expended and the loss of productivity addressing and attempting to mitigate the actual

1 and future consequences of the Data Breach, including but not limited to efforts spent
 2 researching how to prevent, detect, contest, and recover from identity theft; (g) the
 3 continued risk to their PII, which remain in Defendant's possession and is subject to
 4 further unauthorized disclosures so long as Defendant fail to undertake appropriate
 5 and adequate measures to protect customers' PII in their continued possession; and
 6 (h) future costs in terms of time, effort, and money that will be expended to prevent,
 7 detect, contest, and repair the impact of the PII compromised as a result of the Data
 8 Breach for the remainder of the lives of Plaintiff and Class Members.

9 139. As a direct and proximate result of Defendant's breach of their fiduciary
 10 duty, Plaintiff and Class Members have suffered and will continue to suffer other
 11 forms of injury and/or harm, and other economic and non-economic losses.

12 **TENTH CAUSE OF ACTION**

13 **Injunctive/Declaratory Relief**

14 (On Behalf of the Nationwide Class Against Defendant)

15 140. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

16 141. This Count is brought under the federal Declaratory Judgment Act, 28
 17 U.S.C. §2201.

18 142. As previously alleged, Plaintiff and Class Members entered into an
 19 implied contract that required Defendant to provide adequate security for the PII they
 20 collected from Plaintiff and Class Members.

21 143. Defendant owes a duty of care to Plaintiff and Class Members requiring
 22 them to adequately secure PII.

23 144. Defendant still possesses PII regarding Plaintiff and Class Members.

24 145. Since the Data Breach, Defendant has announced few if any changes to
 25 its data security infrastructure, processes or procedures to fix the vulnerabilities in its
 26 computer systems and/or security practices which permitted the Data Breach to occur
 27 and, thereby, prevent further attacks.
 28

1 146. Defendant has not satisfied their contractual obligations and legal duties
2 to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security
3 is known to hackers, the PII in Defendant's possession is even more vulnerable to
4 cyberattack.

5 147. Actual harm has arisen in the wake of the Data Breach regarding
6 Defendant's contractual obligations and duties of care to provide security measures to
7 Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of
8 additional or further harm due to the exposure of their PII and Defendant's failure to
9 address the security failings that lead to such exposure.

10 148. There is no reason to believe that Defendant's security measures are any
11 more adequate now than they were before the Data Breach to meet Defendant's
12 contractual obligations and legal duties.

13 149. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing
14 security measures do not comply with their contractual obligations and duties of care
15 to provide adequate security, and (2) that to comply with their contractual obligations
16 and duties of care, Defendant must implement and maintain reasonable security
17 measures, including, but not limited to, the following:

- 18 a. Ordering that Defendant engage third-party security
19 auditors/penetration testers as well as internal security personnel to
20 conduct testing, including simulated attacks, penetration tests, and
21 audits on Defendant's systems on a periodic basis, and ordering
22 Defendant to promptly correct any problems or issues detected by
23 such third-party security auditors;
- 24 b. Ordering that Defendant engage third-party security auditors and
25 internal personnel to run automated security monitoring;
- 26 c. Ordering that Defendant audit, test, and train their security personnel
27 regarding any new or modified procedures;
- 28

- d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant not transmit PII via unencrypted email;
- f. Ordering that Defendant not store PII in email accounts;
- g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;
- h. Ordering that Defendant conduct regular computer system scanning and security checks;
- i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter a judgment awarding the following relief:

- a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;
- b. Injunctive relief requiring Defendant to (1) strengthen their data security systems that maintain personally identifying information to comply with

the applicable state laws alleged herein (including, but not limited to, the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

- c. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;
- d. An award to Plaintiff and all Nationwide Class members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;
- e. An award to Plaintiff and all Nationwide Class members credit monitoring and identity theft protection services;
- f. An award of attorneys' fees, costs, and expenses, as provided by law or equity;
- g. An order requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law or equity; and
- h. Such other or further relief as the Court may allow.

Dated: January 25, 2024

Respectfully submitted,

BARRACK, RODOS & BACINE

/s/ Stephen R. Basser

Stephen R. Basser

sbasser@barrack.com

Samuel M. Ward

sward@barrack.com

BARRACK, RODOS & BACINE

1 One America Plaza
2 600 West Broadway, Suite 900
3 San Diego, CA 92101
4 Telephone: (619) 230-0800

5 Bruce W. Steckler *
6 bruce@swclaw.com
7 **STECKLER WAYNE CHERRY &**
8 **LOVE, PLLC**
9 12720 Hillcrest Road
10 Dallas, Texas 75230
11 Telephone: (972) 387-4040
12 Facsimile: (972) 387-4041

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
*application for admission *Pro Hac Vice*
forthcoming

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: January 26, 2024

Respectfully submitted,

BARRACK RODOS & BACINE

/s/ Stephen R. Basser

Stephen R. Basser

sbasser@barrack.com

Samuel M. Ward

sward@barrack.com

BARRACK, RODOS & BACINE

One America Plaza

600 West Broadway, Suite 900

San Diego, CA 92101

Telephone: (619) 230-0800

Bruce W. Steckler *

bruce@swclaw.com

**STECKLER WAYNE CHERRY &
LOVE, PLLC**

12720 Hillcrest Road

Dallas, Texas 75230

Telephone: (972) 387-4040

Facsimile: (972) 387-4041